REMARKS

Claims 1-32 are pending in this application and stand rejected by the examiner. Claims 1 and 30-32 are independent claims. Assignee traverses the rejections.

Claim Rejections – 35 U.S.C. § 112

Claims 1, 3, 5, 8-10, 12, 16-18, 20, 21, 24, 25, 28, 29, and 31 stand rejected in the office action under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The office action maintains that there is insufficient antecedent basis for the limitation "the remote device" and noted that there is a plurality of remote devices in claim 1. Assignee respectfully disagrees with the instant rejection, however in order to expedite prosecution of the application, assignee has amended independent claims 1 and 31 to refer to a remote device.

The office action provides a rejection of claim 3 based upon the limitation "the received access code" as having insufficient antecedent basis for this limitation in the claim. Claim 3 has been amended herein to address the antecedent basis rejection.

The office action provides a rejection of claims 7, 9, and 21 based upon the limitation "the user" as having insufficient antecedent basis for this limitation in the claims. Assignee respectfully submits that the amendment to claim 1 addresses the instant rejection. Moreover, the context surrounding the term "the user" in these claims removes any ambiguity about which user is being referred to (e.g., in claim 7, the term "the user" is modified by the participial phrase "requesting the authentication information).

The office action provides a rejection of claims 13 and 15 based upon the term "short" as being a relative term which renders the claim indefinite. Assignee respectfully disagrees with

the instant rejection, however in order to expedite prosecution of the application, assignee has amended claims 13 and 15 to remove the term "short" from the claims.

With these amendments and remarks, assignee respectfully submits that the instant rejections have been traversed and the claims should be allowed.

Claim Rejections – 35 U.S.C. §§ 101

Claims 1-29 and 31 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The office action maintains that claims 1-29 and 31 disclose a system comprising an authentication information store and authentication system, which in light of the specification, appear to be software modules, which do not fall within any of the four categories of invention. Assignee respectfully disagrees, however in order to expedite prosecution of this application, limitations have been added independent claims 1 and 31 to address the instant rejection. With these amendments, assignee respectfully submits that the instant rejections have been traversed and that the claims should be allowed.

Claim Rejections – 35 U.S.C. §§ 103

Claims 1-32 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Owen et al. (2004/0187018). These rejections are traversed.

Claim 1 is directed to a system for distributing authentication information to users of remote devices. Claim 1 recites in combination with its other limitations that an authentication information store stores authentication information for users, and that the authentication system *retrieves the authentication information* for one of the plurality of users from the authentication information store. The *retrieved authentication information* is provided to the remote device.

The office action rejects claim 1 based upon Owen. On page 4, the office action equates the user's authentication information (of claim 1) with the "encrypted passcode" of Owen (emphasis in the original):

> e. wherein the retrieved authentication information is provided to the remote device for use in authenticating a user that is requesting remote access to computer network (ie. *communicate encrypted passcode to the suspect user for presentation to the access authority*) [page 2, paragraph 0010].

Assignee respectfully disagrees with this equating/mapping contained in the office action. Owen does not disclose that authentication information retrieved from a data store is the authentication information that is sent to the remote device as required by claim 1. Owen does not retrieve the "encrypted passcode" from a data store. Rather, Owen "generates (Step 518) a passcode," and "then encrypts (Step 524) the ... passcode," and "communicates (Step 526) the encrypted passcode over the ancillary communications network to the suspect user." (See, Owen at paragraph [0076].) Accordingly, Owen makes clear that the passcode is generated in response to a request, and thus is not stored in a pre-existing data store for retrieval and sending to a remote device as required by claim 1.

To further illustrate the differences from Owen, claim 1 recites that the authentication information store stores the authentication information (which is the information to be sent to the remote device). Owen, instead, has stored "the PIN of the authorized user" (which is not transmitted in Owen to the remote device) in order to compare "(Step 516) the decrypted suspect PIN with the PIN of the authorized user that is retrieved based on the primary ID of the passcode request." (See, Owen at paragraph [0076].) Figure 1 of Owen makes this clear that such data is never transmitted from the server (authentication authority 130) over the network to the suspect user 110 (but instead, a generated passcode is the transmitted information). This is in stark

contrast to claim 1, which requires retrieving authentication information from a store and sending it to the remote device.

In addition to the reasons mentioned above, information such as a PIN would not be transmitted in Owen from the authentication authority to the suspect user because the suspect user already has this information in order to access the authentication authority in the first place. (See the "Suspect PIN" data flow on Figure 1 of Owen.) Because of such differences from Owen, claim 1 is patentable over Owen and therefore should be allowed. Because claim 1 is allowable, its dependent claims are also allowable.

In rejecting the other independent claims, the office action cites Owen as disclosing the subject matter recited in independent claims 30-32. Assignee respectfully disagrees. In these claims, the user provides a request for the authentication information that is stored in an authentication data store. After authentication of the user, the authentication information (that is stored in the data store) is returned to the remote device so that the remote device may access computer resources based upon the returned authentication information. Owen does not disclose such limitations. As shown above, Owen never discloses that, when a user is attempting to access a remote computer resource (e.g., a computer network), authentication information from an authentication information store is transmitted to a remote device. Because Owen discloses such a different approach than the respective subject matter in claims 30-32, these claims are allowable and should proceed to issuance.

[Continued on the next page]

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

Date: July 18, 2008

By: 

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point; 901 Lakeside Avenue
Cleveland, OH 44114
(216) 586-3939